

In the Claims

The status of claims in the case is as follows:

- 1 1. [Previously presented] Method for operating a first
2 node in a network including at least one second node,
3 comprising the steps of:
- 4 establishing at said first node a coincident endpoint
5 for an outer connection and an inner connection with
6 respect to at least one second node, said outer
7 connection and said inner connection being IP security
8 connections;
- 9 responsive to receiving an inbound nested packet from
10 said second node on said outer connection,
11 decapsulating said packet into a first packet and then
12 performing source-in network address translation on
13 said first packet; and
- 14 responsive to receiving an outbound second packet at
15 said inner connection, performing source-in network
16 address translation on said second packet, and then
17 encapsulating said second packet into a nested packet
18 for communication on said outer connection to said
19 second node.

2. [Canceled]

END920000093US1

3

S/N 09/813,910

1 3. [Currently amended] Method for managing nested
2 connections having a coincident endpoint within a
3 communications system, comprising the steps of:

4 configuring an outer IP security connection;

5 communicating from a client to a gateway on said outer
6 connection a request to configure a secure inner
7 connection having said coincident endpoint with said
8 outer connection;

9 responsive to said request, initializing said gateway
10 to receive a future nested communication, including
11 obtaining a client address from a packet on said outer
12 connection;

13 starting said inner connection;

14 responsive to starting said inner connection,
15 propagating a network address translation rule from
16 said outer connection to said inner connection.

1 4. [Original] The method of claim 3, further comprising
2 the step of:

3 further responsive to starting said inner connection,
4 encapsulating a packet outbound from said gateway first
5 in said inner connection and then in said outer
6 connection.

END920000093US1

4

S/N 09/813,910

1 5. [Original] The method of claim 4, further comprising
2 the steps of:

3 responsive to receiving a packet at said gateway,
4 determining if said packet has a security header;

5 responsive to said packet having said security header,
6 decapsulating said packet and saving any address
7 translation rule included within said packet; and

8 applying said address translation rule to said packet
9 and thereafter communicating said packet from said
10 gateway to said client.

1 6. [Original] The method of claim 5, further comprising
2 the steps of:

3 iteratively executing said decapsulating step until a
4 resulting decapsulated packet no longer contains a
5 security header.

1 7. [Previously presented] Method for enabling a local
2 gateway to handle dynamically assigned IP addresses from
3 remote clients, comprising the steps of:

4 assigning said IP address to a remote client;

END920000093US1

5

S/N 09/813,910

5 automatically maintaining between said remote client
6 and said gateway nested IP security connections with
7 local coincident endpoints.

1 8. [Original] The method of claim 7, wherein said nested
2 connections comprise an inner connection and an outer
3 connection.

1 9. [Previously presented] The method of claim 8, further
2 comprising the steps of:

3 responsive to receiving an inbound nested packet from
4 said client on said outer connection, decapsulating
5 said packet into a first packet and then performing
6 source-in network address translation on said first
7 packet; and

8 responsive to receiving an outbound second packet at
9 said inner connection, performing source-in network
10 address translation on said second packet, and then
11 encapsulating said second packet into a nested packet
12 for communication on said outer connection to client.

1 10. [Previously presented] System for operating a first
2 node in a network including at least one second node,
3 comprising:

4 an inner IP security connection;

END920000093US1

6

S/N 09/813,910

5 an outer IP security connection;

6 a local coincident endpoint for said outer connection
7 and said inner connection at said first node with
8 respect to at least one second node;

9 said first node being responsive to receiving an
10 inbound nested packet from said second node on said
11 outer connection for decapsulating said packet into a
12 first packet and then performing source-in network
13 address translation on said first packet; and

14 said first node being further responsive to receiving
15 an outbound second packet at said inner connection for
16 performing source-in network address translation on
17 said second packet, and then encapsulating said second
18 packet into a nested packet for communication on said
19 outer connection to said second node.

1 11. [Currently amended] Method for extending virtual
2 private network (VPN) network address translation (NAT) to
3 include support for nested connections with coincident
4 endpoints, without requiring any special configuration for
5 the inner (nested) VPN connection, with respect to VPN NAT,
6 comprising the steps of:

7 configuring an outer IP security connection with a VPN
8 NAT rule;

END920000093US1

7

S/N 09/813,910

9 communicating from a client to a gateway on said outer
10 connection a dynamically generated security association
11 request packet to configure a secure inner connection;

12 responsive to said request, initializing said gateway
13 to receive a future nested communication, including
14 obtaining a client address from said request packet on
15 said outer connection;

16 starting said inner connection;

17 responsive to starting said inner connection,
18 propagating said VPN NAT rule from said outer
19 connection to said inner connection, said inner and
20 outer connections having a coincident endpoint.

1 12. [Original] The method of claim 11, further comprising
2 the step of:

3 further responsive to starting said inner connection,
4 encapsulating a packet outbound from said gateway first
5 in said inner connection and then in said outer
6 connection.

1 13. [Original] The method of claim 12, further comprising
2 the steps of:

3 responsive to receiving a packet at said gateway,
4 determining if said packet has a security header;

END920000093US1

8

S/N 09/813,910

5 responsive to said packet having said security header,
6 decapsulating said packet and saving any VPN NAT rule
7 included within said packet; and

8 applying said NAT rule to said packet and thereafter
9 communicating said packet from said gateway to said
10 client.

1 14. [Original] The method of claim 13, further comprising
2 the step of:

3 iteratively executing said decapsulating step until a
4 resulting decapsulated packet no longer contains a
5 security header.

1 15. [Canceled]

2 16. [Currently amended] System for extending virtual
3 private network (VPN) network address translation (NAT) to
4 include support for nested connections with coincident
5 endpoints, without requiring any special configuration for
6 the inner (nested) VPN connection, with respect to VPN NAT,
7 comprising:

8 a gateway;

9 a client;

10 an inner IP security connection for connecting said

END920000093US1

9

S/N 09/813,910

11 gateway and said client;

12 an outer IP security connection for connecting said
13 gateway and said client;

14 said inner and outer IP security connections including
15 a coincident endpoint;

16 said outer connection being configured by said client
17 with a VPN NAT rule;

18 said outer connection for communicating from said
19 client to said gateway a dynamically generated security
20 association request packet to configure said inner
21 connection;

22 said gateway further responsive to said request for
23 initializing said gateway to receive a future nested
24 communication, including obtaining a client address
25 from said request packet on said outer connection;

26 said gateway further responsive to starting said inner
27 connection for propagating said VPN NAT rule from said
28 outer connection to said inner connection.

1 17. [Previously presented] A program storage device
2 readable by a machine, tangibly embodying a program of
3 instructions executable by a machine to perform method steps
4 for operating a first node in a network including at least

END920000093US1

10

S/N 09/813,910

5 one second node, said method steps comprising:

6 establishing at said first node a coincident endpoint
7 for an outer connection and an inner connection with
8 respect to at least one second node, said outer
9 connection and said inner connection being IP security
10 connections;

11 responsive to receiving an inbound nested packet from
12 said second node on said outer connection,
13 decapsulating said packet into a first packet and then
14 performing source-in network address translation on
15 said first packet; and

16 responsive to receiving an outbound second packet at
17 said inner connection, performing source-in network
18 address translation on said second packet, and then
19 encapsulating said second packet into a nested packet
20 for communication on said outer connection to said
21 second node.

1 18. [Previously presented] A computer program product or
2 computer program element for operating a first node in a
3 network including at least one second node according to the
4 steps of:

5 establishing at said first node a coincident endpoint
6 for an outer connection and an inner connection with
7 respect to at least one second node, said outer

END920000093US1

11

S/N 09/813,910

8 connection and said inner connection being IP security
9 connections;

10 responsive to receiving an inbound nested packet from
11 said second node on said outer connection,
12 decapsulating said packet into a first packet and then
13 performing source-in network address translation on
14 said first packet; and

15 responsive to receiving an outbound second packet at
16 said inner connection, performing source-in network
17 address translation on said second packet, and then
18 encapsulating said second packet into a nested packet
19 for communication on said outer connection to said
20 second node.

1 19. [Currently amended] A program storage device readable
2 by a machine, tangibly embodying a program of instructions
3 executable by a machine to perform method steps for managing
4 nested connections with a coincident endpoint within a
5 communications system, said method steps comprising:

6 configuring an outer IP security connection;

7 communicating from a client to a gateway on said outer
8 connection a request to configure a secure inner
9 connection;

10 responsive to said request, initializing said gateway

END920000093US1

12

S/N 09/813,910

11 to receive a future nested communication, including
12 obtaining a client address from a packet on said outer
13 connection;

14 starting said inner connection;

15 responsive to starting said inner connection,
16 propagating a network address translation rule from
17 said outer connection to said inner connection.

1 20. [Original] The storage device of claim 19, said method
2 steps further comprising the step of:

3 further responsive to starting said inner connection,
4 encapsulating a packet outbound from said gateway first
5 in said inner connection and then in said outer
6 connection.

1 21. [Original] The storage device of claim 20, said method
2 steps further comprising the steps of:

3 responsive to receiving a packet at said gateway,
4 determining if said packet has a security header;

5 responsive to said packet having said security header,
6 decapsulating said packet and saving any address
7 translation rule included within said packet; and

8 applying said address translation rule to said packet

END920000093US1

13

S/N 09/813,910

9 and thereafter communicating said packet from said
10 gateway to said client.

1 22. [Original] The storage device of 21, said method steps
2 further comprising the steps of:

3 iteratively executing said decapsulating step until a
4 resulting decapsulated packet no longer contains a
5 security header.

END920000093US1

14

S/N 09/813,910